Information & Computer Security

Towards a framework for the potential cyber-terrorist threat to critical national infrastructure: A quantitative study

Abdulrahman Alqahtani

Received 9 September 2014
Revised 13 November 2014
7 December 2014
28 February 2015
Accepted 4 March 2015

Towards a framework for the potential cyber-terrorist threat to critical national infrastructure

A quantitative study

Abdulrahman Alqahtani
School of Politics, Philosophy and International Studies, Hull University, Hull, UK

Abstract

Purpose – The main purpose of this research is to produce the most accurate theoretical framework of the potential threat of cyberterrorism to the national security, compared to conventional terrorism. So it aims to identify the theoretical framework that best explains the threat of cyberterrorism and conventional terrorism to national security derived from empirical data, using grounded theory, and to validate the developed grounded theory statistically by quantitative data.

Design/methodology/approach – This paper presents the results of the quantitative study survey. It provides in the beginning basic information about the data. To purify the data, reliability and exploratory factor analysis, as well as confirmatory factor analysis (CFA), were performed. Then, structural equation modelling was utilised to test the final model of the theory and to assess the overall goodness-of-fit between the proposed model and the collected data set.

Findings – The first study, as a qualitative exploratory study, gives a rich data set that provides the foundation of the development of the second study, as a quantitative confirmatory study. In the researcher's previous qualitative study, it provides a better theoretical understanding of the potential threat of cyber and conventional terrorism to Saudi national security. Also, it provides the development of the grounded theory of the study (Figure 1). It also has led to the development of the conceptual framework and the hypotheses for the second phase of the study (i.e. survey).

Originality/value – It is original study based on empirical data collected from Saudi military and security officials and experts in the critical infrastructures.

Keywords Information security modeling, National security, Terrorism, Critical infrastructure, Cyberterrorism

Paper type Research paper

Introduction

During the history of mankind, there have been many events and dangers that have threatened the security of states. Those threats caused heavy loss of life, the spread of disease, injuries, destruction of public and private property, displacement of large numbers of people and heavy economic losses. Political unrest at international and local levels, and recent technological developments, are elements that would increase the seriousness of threats against national security (Inoguchi, 1996).

The concept of security has evolved gradually, but, more particularly, after the major international transformation brought about by the disintegration of the Soviet Union and the end of the Cold War. This left behind a bipolar world, which gave a blurred image of relationships between states and made them ambiguous. Simultaneously,

Information & Computer Security
Vol. 23 No. 5, 2015
pp. 532-569

2056-4961
DOI 10.1108/ICS-09-2014-0060

globalisation has changed international rules and norms to facilitate the rapid flow of capital and technology, through the weakening of national barriers. Non-governmental actors have come to play an essential role in international politics, some of them as a threat, and others to bridge the gap between communities and nations. In such circumstances, the role of the state has begun to suffer from the changes; also, the accepted traditional concept of power has been challenged (Tadjbakhsh and Chenoy, 2007).

Today, there are no issues of such concern worldwide, arousing such a high degree of hot debate at both national and international levels, as terrorism-related issues. The threat of terrorism has never been as prominent as it seems to be at the present time. Terrorism is an old phenomenon that has existed since the emergence of human societies. However, the threat of terrorism has increased steadily over the past 30 years. With the technological and technical progress in various areas, the actions of terrorists have become more dangerous and destructive, as the perpetrators of such acts are becoming more elusive. There are few parts of the world that have been spared the current waves of terrorism, which started in the late 1960s (Mythen and Walklate, 2006). The phenomenon of terrorism is changing, while the general motives of terrorism remain the same, to pursue their policies. The world today faces new and unfamiliar kinds of weapons. The international system, intelligence systems, security procedures and tactics which are expected to protect people, nations and governments, are not able to meet this new and devastating enemy. The methods and strategies that have been developed to combat terrorism over the years are relatively ineffective in the face of this enemy. The reason for this is that the enemy no longer attacks with just hijacked planes, truck bombs or suicide bombers strapped with explosives. The enemy attacks with ones and zeros. This is the weak point, the integration of the virtual worlds with the physical worlds. It is cyber-terrorism (Collin, 2013).

Terrorism has passed historically through many phases and waves, and as a strategy used to achieve certain goals, terrorism uses the tools and possible means available in every time and place. Even the 9/11 attacks on the World Trade Centre, using hijacked planes to collide into buildings and blow them up, is considered a major shift in terrorism strategy. More than just creating a state of terror and intimidation of a particular community in a specific place, terrorism has become aimed at creating a state of chaos, terror and intimidation at an international level. Consequently, this event caused an irreversible change in the procedures for international travel.

The modern world lives in the digital age; some call it the information age and some go beyond that to denote it as the knowledge and intelligence era (Rowe *et al.*, 1996, pp. 4-6). Societies in most countries of the world have become permanently dependent on electronic devices and networks to manage almost everything, from just surfing the Internet and controlling networks of water and sanitation to surgical procedures and space exploration. Therefore, an attack on these networks and systems to achieve political goals is nothing but a kind of terrorism. Despite the fact that the immediate victims are computers and networks, the general public ultimately are the victim in this whole matter. This issue must be addressed by politicians, security agencies and leaders, and not thrown haphazardly onto the departments of information and communication technology, on the pretext that it is a technical issue difficult to understand and embrace.

Such issues are of growing concern in Saudi Arabia, one of the developing countries characterised by very rapid development in both the economy in general, and in the critical infrastructure of communications and information networks. This enormous development coincides with increasing reliance on these networks and communications to provide basic services needed by the people and the government on a daily basis. The national security of Saudi Arabia, or of any state, aims to achieve safety and stability and is based on several elements, including the political system, the government, and the critical infrastructure. These elements work together to achieve the well-being of the people and the state. Because these elements rely on computer systems and networks for control, management, operations and communications, any defect or paralysis caused by malicious acts of cyberterrorism would be very costly and offensive to state organisations, and thus, such acts are considered a potential direct threat to national security.

National security is a very important priority and a highlighted concern; the interest it receives increases or weakens based on the increase or decrease in potential threats. So, national security can be enhanced by harnessing all the overall powers of the state, which include political, technological and economic power, military strength and power management. The legitimacy and effectiveness of the state leadership depends to a great extent on their ability to eliminate national security risks, and achieve the security and well-being of its people. From this standpoint, Saudi Arabia is striving locally, regionally and globally to achieve national security and consolidate security and stability, through its saving energy in the global market and keeping oil prices stable. In this situation, any potential threat to the national security of Saudi Arabia, given current international relations and international connectivity, may also affect global security, which may result in the destabilisation of international oil prices, consequent economic damage and political tension. Given that Saudi Arabia actively pursues the development of critical infrastructure, along the lines of the developed world, and relies increasingly on computer systems and networks in government organisations, oil companies, banking, technology services, communications, water and sanitation and other areas, there exist opportunities and potential threats that could be exploited by terrorist organisations to launch cyber-attacks to disrupt and disable these services.

Saudi Arabia, having suffered for some time from conventional terrorism, has adopted procedural policies to confront it, but the possibility of conventional terrorism turning to cyber-terrorism has left a security and legislative gap, either because the government is not aware of the dangers and vulnerabilities or it is not prepared for a response.

Given the scenario outlined above, the following questions arise.

Research objectives

The main objective of this study is to test the validation of the proposed theoretical framework of the potential terrorist threats to national security. This objective can be achieved by obtaining the necessary data from critical infrastructure sectors, which are among the key elements of national security.

The benefit derived from this study is that critical infrastructure will be fully aware of the threats posed by cyber-terrorism, be fully knowledgeable of their vulnerabilities, and have the appropriate response in case of any cyber-terrorist attacks. This, in turn, will help to reduce the physical and moral effects which are the main objective of terrorism. It will also allow adequate opportunity for decision-makers in crisis management to make decisions, based on a full knowledge of the real situation, about the components of critical infrastructure and the general public.

Research importance

Information and communication technology heightened the importance and interest in the spread and exchange of information between the continents and countries of the world, and has therefore become one of the pillars of the current era, bringing with it many benefits. Nevertheless, it has raised risks and security concerns. With the entry of the Web or "Internet" and the ever-increasing numbers of users of this technology, terrorist attackers, hackers and intruders spend hours in attempts to penetrate, or gain access to, important information which can be used for material and moral extortion.

Given the importance of the security of the constantly evolving critical infrastructure in Saudi Arabia, and its related networks, information systems, control systems and supervision, as well as the importance of information security to the general public, this is one of the major and important factors to achieve and maintain national security in Saudi Arabia. In contrast, any disruption or instability in national security will result in very serious consequences for the stability of the country, its economy and its political situation.

This research derives its significance from the importance of its themes. Saudi Arabia's national security is of top priority to the Saudi Government. Understanding, identifying and predicting early indicators that may pose a threat to national security will make it easier to achieve good national security in the country.

The pairing and comparison between cyber and conventional terrorism will help to identify the levels of knowledge, awareness, vulnerabilities, response and impact of the threats. This, in turn, will provide a conceptual framework for decision-makers about the problem in question and therefore the government will be able to take the necessary action on a clear basis and within a strategic path to combat cyber-terrorism.

Also, this study departs somewhat from previous terrorism studies, as an analysis of the literature on terrorism, conducted in 2006, revealed that 96 per cent of terrorism studies were "think pieces"; only 3 per cent had an empirical basis; and only 1 per cent were case studies (Schmid, 2011, p. 461). This is an indicator of severe shortages of empirical and case studies in the field of terrorism. This study is an attempt to contribute to fill this gap in terrorism studies. By studying Saudi Arabia, it is contributing another case study to the overall discourse on cyberterrorism.

Conceptual framework and study hypotheses

A previous study conducted by the researcher provided the development of the grounded theory of the study (Figure 1). This has also led to the development of the conceptual framework and the hypotheses for the second phase of the study (i.e. survey).

Figures 2 and 3 show the conceptual framework of the study based on the grounded theory, resulting from the qualitative study in the first phase of this research.

As the quantitative study is here to validate the resulting grounded theory from the previous study, the hypothesis of this study is to prove the validity of the relationships

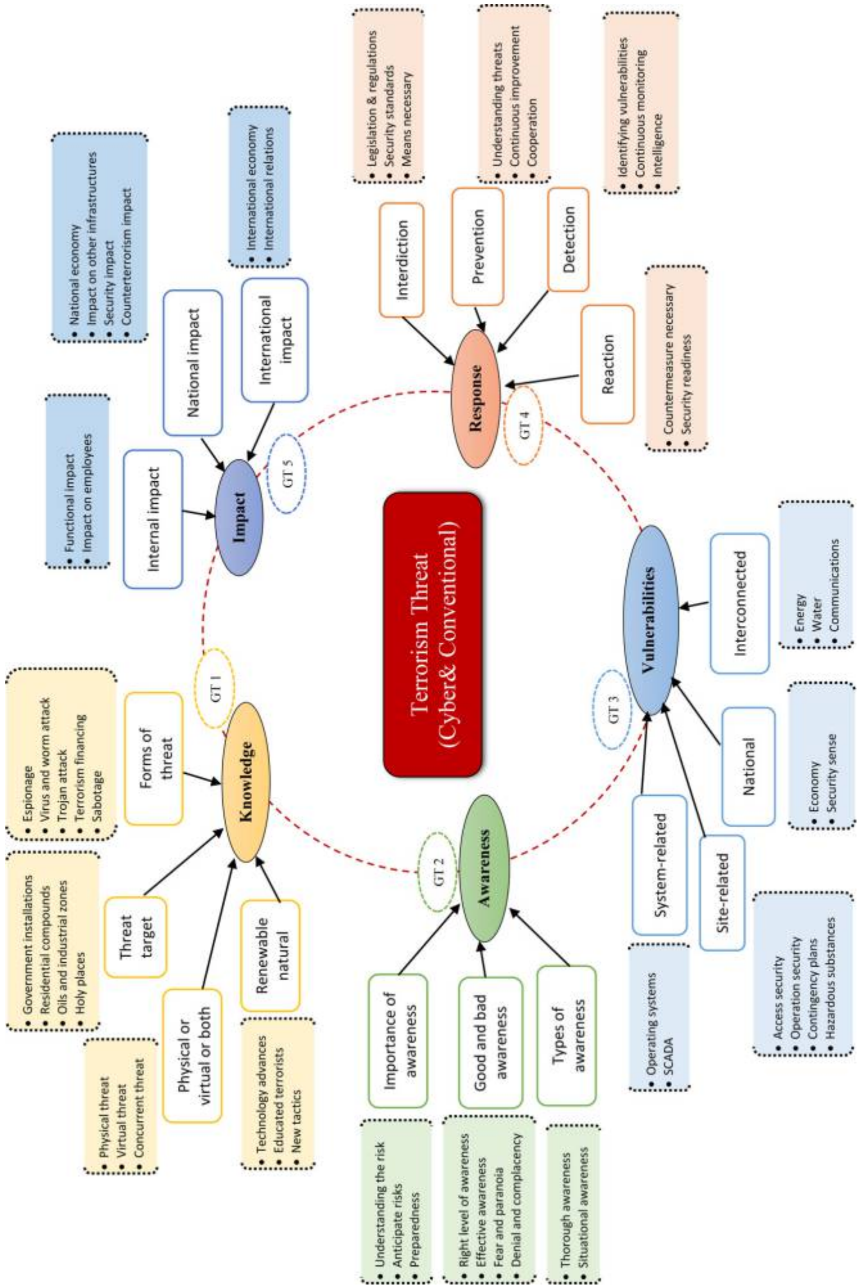

Figure 1.
Grounded theory categories

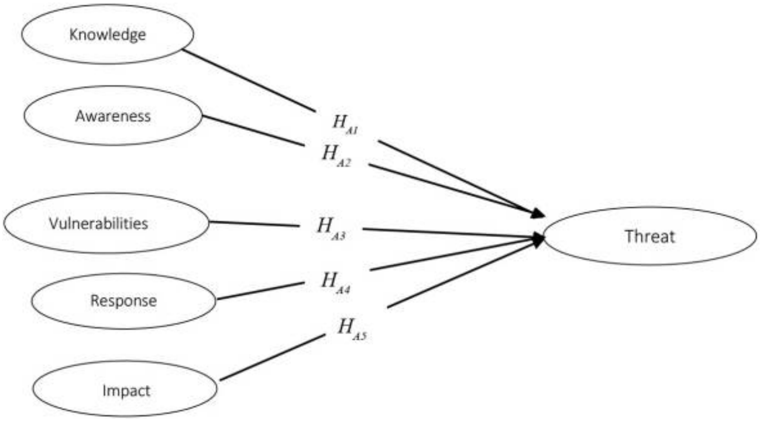

Figure 2.
Study conceptual framework (Cyberterrorism)

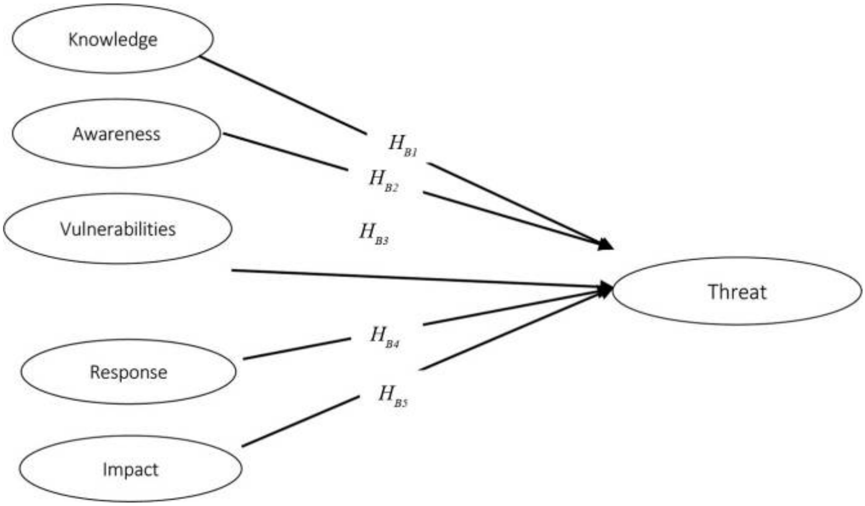

Figure 3.
Study conceptual framework (Conventional terrorism)

between the constructs in the conceptual framework. A summary of the study's hypothesised relationships based on the grounded theory is provided below:

- H_A. The conceptual framework (Grounded theory) for cyberterrorism will be statistically valid.
- H_{A1}. Knowledge of cyberterrorism will be highly related to identifying the threat.
- H_{A2}. Awareness of cyberterrorism will be highly related to identifying the threat.
- H_{A3}. Vulnerabilities of cyberterrorism will be highly related to identifying the threat.
- H_{A4}. Response to cyberterrorism will be highly related to identifying the threat.
- H_{A5}. Impact of cyberterrorism will be highly related to identifying the threat.

H_B. The conceptual framework (Grounded theory) for conventional terrorism will be statistically valid.

H_{B1}. Knowledge of conventional terrorism will be highly related to identifying the threat.

H_{B2}. Awareness of conventional terrorism will be highly related to identifying the threat.

H_{B3}. Vulnerabilities of conventional terrorism will be highly related to identifying the threat.

H_{B4}. Response to conventional terrorism will be highly related to identifying the threat.

H_{B5}. Impact of conventional terrorism will be highly related to identifying the threat.

Pilot study

In light of the methodology of this study, the second phase (quantitative study) is to prove the validity of the resulting grounded theory from the first phase; the researcher has sought to develop a reliable and valid scale of the theoretical constructs based on this grounded theory. This process follows Churchill's (1979) approach of systematic scale development procedures. The process of scale development followed is shown in Figure 4.

A pilot study was carried out to detect any defects in the questionnaire, such as unclear or misleading questions, or those that may lead to invalid answers. Based on feedback obtained from a panel of academics, the number of items was reduced from 62 to 55. Subsequently, 30 copies of the revised questionnaire were distributed to a selected sample of Saudi students at the University of Hull, and 27 questionnaires were returned. Five items were omitted from the questionnaire based on comments provided by the pilot study sample. Table I illustrates these items and the reasons for dropping them.

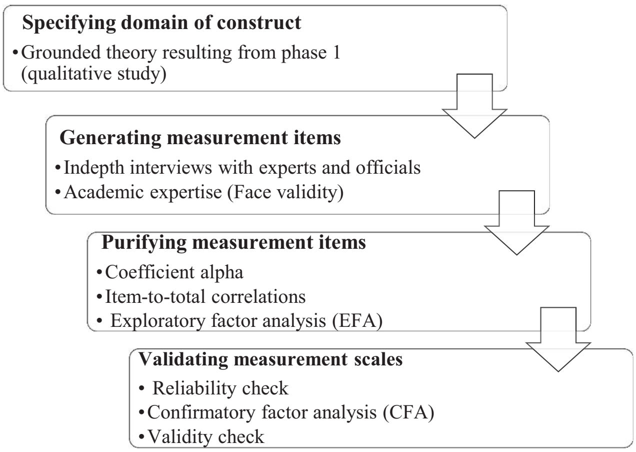

Figure 4.
Measurement scales development steps

Item no.	Items dropped	Reasons for dropping the items
10	Knowledge of the most likely threat against the organisation: either cyber or conventional terrorism, or both	Panel-overlap with another item
11	Continuous monitoring for news of terrorist events at the local and international level	Panel-overlap with another item
13	Knowledge of conventional terrorist attack methods, such as bombings, assassinations and kidnappings, etc	Panel-overlap with another item
14	Knowledge of techniques and methods of cyber-attacks, such as the types of viruses, worms, hackers etc	Panel-overlap with another item
23	Existing awareness of the need to predict the potential security risks against the organisation	Sample – incomprehensible
47	Organisation makes security a priority, in the face of conventional terrorist attacks	Sample – incomprehensible
48	Organisation makes security a priority, in the face of cyber terrorist attacks	Sample – incomprehensible
50	Organisation dependency on competent security authorities, in the event of terrorist attacks	Panel-overlap with another item
53	Partial defect of some of the organisation's activities in the case of exposure to conventional terrorist attacks	Panel-overlap with another item
54	Partial defect of some of the organisation's activities in the case of exposure to cyber terrorist attacks	Panel-overlap with another item
61	Conventional terrorist attacks have a great impact in general, on the organisation	Sample – incomprehensible
62	Cyber terrorist attacks have a great impact in general, on the organisation	Sample – incomprehensible

Table I. Items dropped in the pilot study and the reasons

Also, some items were reworded more clearly because they were translated from the Arabic. There were also minor adjustments in the order of items and formatting. This was all to make it ready for the main survey.

Main survey

Data set

After the distribution of the questionnaires and the follow-up, the researcher received 537 questionnaires from staff in the departments of information technology and security in the critical infrastructure sector. This response represents a response rate of 46.6 per cent, which is good for the study. Also, while the researcher was entering the questionnaires' data into SPSS, he performed screening on the questionnaires, by eye, in terms of completeness and quality for analysis. As a result, 21 questionnaires were excluded due to the low number and quality of answers. Consequently, the number of valid questionnaires for analysis was 516. Table II presents the demographic characteristics of the respondents. Results showed that the majority of respondents work in the governmental sector (69.4 per cent). The majority are aged between 20 and 30 years (66 per cent), while only two are less than 20 years old, and 15 are older than 50 years old. The majority also hold a Bachelor's degree or technical or military training, while only 3 hold doctoral degrees.

Characteristics	*N*	(%)
Sector		
Governmental	358	69.4
Private sector	158	30.6
Total	516	100.0
Age		
Less than 20 years	2	0.4
From 20 to less than 30 years	344	66.7
From 30 to less than 40 years	120	23.3
From 40 to less than 50 years	36	7.0
50 years and over	14	2.7
Total	516	100.0
Rank or grade		
Grade 5 or less	44	8.5
Grade 6 to 9	146	28.3
Grade 10 and above	36	7.0
Non-commissioned officer	193	37.4
Lieutenant to captain	72	14.0
Major and above	25	4.8
Total	516	100.0
Service years		
Less than 5 years	186	36.0
From 5 to less than 10 years	175	33.9
From 10 to less than 15 years	118	22.9
From 15 to less than 20 years	29	5.6
20 years and over	8	1.6
Total	516	100.0
Qualification		
Other[a]	193	37.4
Secondary education	44	8.5
Technical training	113	21.9
Bachelor	141	27.3
Master	22	4.3
Doctorate	3	0.6
Total	516	100.0
Specialisation		
Engineering and Natural Sciences	36	7.0
Military and Security Sciences	225	43.6
Management Sciences and Economics	22	4.3
Humanities and Social Sciences	120	23.3
Technical and Vocational Training	113	21.9
Total	516	100.0
Total	516	100.0

Note: [a] Others: military and security training

Table II.
Demographic profile of survey sample ($N = 516$)

Reliability and exploratory factor analysis

The researcher carried out two methods of analysis to purify the scale, reliability and exploratory factor analysis (EFA).

Reliability analysis

Assessing the reliability of internal consistency is the first step in the assessment of multi-scale items to avoid extra dimensions resulting from factor analysis due to rubbish items (Churchill, 1979). The internal consistency of the scale is an important property of the measurement because it means that the items of the scale, despite their distinctiveness and specificity, share a common core and measure the same concept (Anderson and Gerbing, 1982; Netemeyer *et al.*, 2003, p. 46). To assess the internal consistency of the scales, the researcher measured the coefficient alpha for all scales, according to Churchill (1979). The coefficient alpha is concerned with the degree of interrelatedness among sets of items intended to measure a single construct (Cronbach, 1951; Netemeyer *et al.*, 2003, p. 49). Coefficient alpha and item-to-total correlation for each construct were assessed. The statistical criteria are:

- coefficient alpha above 0.7 (Churchill, 1979; Nunnally, 1978, p. 226); and
- corrected item-to-item correlation above 0.35 (Nunnally and Bernstein, 1994).

Table III shows the results of the reliability test.

Exploratory factor analysis

EFA is a variable reduction technique which determines the number of latent constructs and the underlying factor structure of a set of variables at the initial stage of scale development (Netemeyer *et al.*, 2003). EFA is usually used to explore the possible underlying structure of a set of measured variables, without imposing any prior structure (Child, 1990). Given that the measures of this study are based on the grounded theory resulting from an exploratory qualitative study, the researcher carried out EFA as one of the steps to prove the validity of the theoretical model.

EFA was conducted to examine the factorial structure of the scales and to check the reliability of all scales using SPSS 20.0 for Windows. EFA was performed after checking the data (e.g. errors, missing values, descriptive statistics, etc.)

To extract factors by reducing the number of items, the principle component analysis technique and orthogonal (varimax) rotation were used (Hair *et al.*, 2006, p. 112). To assess the viability of the items' reduction to factors, the researcher tested the following three indicators:

(1) the Kaiser-Meyer-Olkin Measure (KMO) of Sampling Adequacy, which was found to be 0.809 for conventional terrorism observed variables and 0.880 for cyberterrorism observed variables which are above the threshold of 0.6 (Kaiser and Rice, 1974);

(2) Bartlett's Test of Sphericity, which was significant at $p < 0.001$ for both scales' variables (Bartlett, 1954); and

(3) communalities, which were also found to be above 0.5, suggesting satisfactory factorability for all scale items.

Constructs	Items	Corrected item – total correlation	Cronbach's alpha if the items deleted	Cronbach's alpha	Sample size (N)[a]
Conventional terrorism (CO)					
Knowledge	KCO1	0.618	0.923	0.913	516
	KCO2	0.764	0.898		
	KCO3	0.896	0.867		
	KCO4	0.841	0.881		
	KCO5	0.806	0.888		
Awareness	ACO1	0.806	0.968	0.963	516
	ACO2	0.925	0.949		
	ACO3	0.890	0.955		
	ACO4	0.903	0.953		
	ACO5	0.956	0.943		
Vulnerabilities	VCO1	0.618	0.907	0.861	516
	VCO2	0.857	0.685		
	VCO3	0.746	0.795		
Response	RCO1	0.882	0.952	0.961	516
	RCO2	0.925	0.945		
	RCO3	0.940	0.944		
	RCO4	0.842	0.959		
	RCO5	0.863	0.956		
Impact	ICO1	0.629	0.783	0.821	516
	ICO2	0.575	0.806		
	ICO3	0.769	0.714		
	ICO4	0.611	0.790		
Cyberterrorism (CY)					
Knowledge	KCY1	0.858	0.914	0.935	516
	KCY2	0.731	0.938		
	KCY3	0.896	0.907		
	KCY4	0.858	0.915		
	KCY5	0.819	0.922		
Awareness	ACY1	0.816	0.971	0.966	516
	ACY2	0.934	0.953		
	ACY3	0.895	0.959		
	ACY4	0.911	0.957		
	ACY5	0.966	0.947		
Vulnerabilities	VCY1	0.936	0.976	0.978	516
	VCY2	0.923	0.977		
	VCY3	0.921	0.977		
	VCY4	0.955	0.975		
	VCY5	0.939	0.976		
	VCY6	0.895	0.979		
	VCY7	0.909	0.978		

(*continued*)

Table III.
The results of the reliability test

Constructs	Items	Corrected item – total correlation	Cronbach's alpha if the items deleted	Cronbach's alpha	Sample size $(N)^a$
Response	RCY1	0.900	0.960	0.967	516
	RCY2	0.918	0.958		
	RCY3	0.912	0.959		
	RCY4	0.945	0.956		
	RCY5	0.845	0.966		
	RCY6	0.849	0.966		
Impact	ICY1	0.965	0.967	0.957	516
	ICY2	0.940	0.971		
	ICY3	0.927	0.972		
	ICY4	0.924	0.973		
	ICY5	0.909	0.975		

Note: [a]No cases have been removed as all the sample was valid after data screening

Table III.

Also, the researcher assessed the factorial solutions obtained from SPSS, such as item loadings and percentage of variance extracted. So, any item which in its highest factor loading is less than 0.5, or is loading high in more than one factor, should be dropped (Hair *et al.*, 2006). In the next part are summaries of the result of the exploratory factor analysis for each scale.

Conventional terrorism scale. This scale contains 22 items. The calculation of item-to-total correlations showed that all items of all the constructs in this scale were correlated well and were internally consistent, as their item-to-total correlations range from 0.575 to 0.956, which are higher than the threshold value (0.35). When applying EFA, the results showed five clear factorial structures. All the loadings of items were above 0.7 and ranged from 0.745 to 0.965. The KMO Measure of Sampling Adequacy was 0.809, as it remained unchanged. Bartlett's Test of Sphericity was significant at $p <$ 0.001 too. Regarding the internal consistency reliability, Cronbach's alpha ranged from 0.821 to 0.963. In addition, all communalities were acceptable, ranging from 0.584 to 0.974 for all items. Consequently, all previous results showed a satisfactory reduction for each of the variables, and they also showed a satisfactory loading in five clean factors which corresponds to the theoretical constructs based on the grounded theory. In addition, the results of all the items were satisfactory, with none of them requiring exclusion from the scale. Table IV shows the final EFA results of conventional terrorism.

Cyberterrorism scale. In this scale, there are 28 items. When applying EFA, the results showed five clear factorial structures. All the loadings of all the items were above 0.7 and ranged from 0.802 to 0.977. The KMO Measure of Sampling Adequacy was 0.880, as it remained unchanged. Bartlett's Test of Sphericity was significant at ($p < 0.001$) too. Moreover, all communalities were acceptable, ranging from 0.684 to 0.959 for all items. The calculation of item-to-total correlations showed that all items of all constructs in this scale were correlated well and were internally consistent, as their item-to-total correlations ranged from 0.731 to 0.966, which are higher than the threshold value (0.35). With regard to the internal consistency reliability, Cronbach's alpha ranged from 0.935 to 0.978. Accordingly, all previous results showed a satisfactory reduction for each of the variables, they also showed a satisfactory loading in five clean factors which

Table IV. Final EFA results of conventional terrorism scale

Conventional terrorism (CO)								EFA	
Construct	Cronbach's alpha	Item-total correlation		Mean	SD	Final loading	% of variance	CVE[a] (%)	MSA[b]
Knowledge	0.913	KCO1	0.618	4.28	0.550	0.745	74.591	79.953	0.809
		KCO2	0.764	4.27	0.545	0.831			
		KCO3	0.896	3.54	0.732	0.937			
		KCO4	0.841	3.58	0.729	0.885			
		KCO5	0.806	3.62	0.607	0.865			
Awareness	0.963	ACO1	0.806	4.08	0.577	0.852	87.116		
		ACO2	0.925	4.15	0.672	0.944			
		ACO3	0.890	4.17	0.651	0.921			
		ACO4	0.903	4.09	0.686	0.933			
		ACO5	0.956	4.08	0.688	0.965			
Vulnerabilities	0.861	VCO1	0.618	4.30	0.585	0.814	78.341		
		VCO2	0.857	4.53	0.617	0.920			
		VCO3	0.746	4.60	0.610	0.862			
Response	0.961	RCO1	0.882	4.01	0.394	0.919	86.660		
		RCO2	0.925	4.03	0.405	0.941			
		RCO3	0.940	4.00	0.369	0.952			
		RCO4	0.842	4.03	0.375	0.886			
		RCO5	0.863	4.06	0.417	0.906			
Impact	0.821	ICO1	0.629	4.09	0.528	0.792	65.266		
		ICO2	0.575	4.14	0.502	0.749			
		ICO3	0.769	4.32	0.526	0.892			
		ICO4	0.611	4.51	0.500	0.784			

Notes: [a] Cumulative variance extracted; [b] KMO measure of sampling adequacy

corresponds to the theoretical constructs based on the grounded theory. In addition, the results of all the items were satisfactory, with none of them requiring exclusion from the scale. Table V on the following page shows the final EFA results of cyberterrorism.

Confirmatory factor analysis

EFA and confirmatory factor analysis (CFA) are two types of factor analyses (Hair *et al.*, 2006; Pallant, 2010).

EFA is a statistical technique for data reduction. It aims to locate the appropriate structure of the variables under the particular logic factors (Hair *et al.*, 2006). On the other hand, CFA offers a precise method to examine the factorability and validity of measures (Gerbing and Anderson, 1988). CFA is used to confirm prior hypotheses about the relationship between the terms of measurements and the factors assigned to them in the model (Netemeyer *et al.*, 2003, p. 148). In this study, the researcher used CFA to confirm the dimensionality of the constructs of scales evolved from EFA, by examining each construct separately as a unidimensionality (Churchill, 1979). A unidimensionality is one latent property or construct underlying a set of scale items (Anderson *et al.*, 1987).

In this approach, the researcher used SPSS.20 for confirming the unidimensionality of each construct using the principle component technique (Field, 2013; Leech *et al.*, 2008). The

Construct	Cronbach's alpha	Item-total correlation		Mean	SD	Final loading	% of variance	EFA CVE[a] (%)	MSA[b]
	Cyberterrorism (CY)								
Knowledge	0.935	KCY1	0.858	3.56	0.731	0.913	79.806	87.438	0.880
		KCY2	0.731	4.27	0.544	0.802			
		KCY3	0.896	3.54	0.735	0.943			
		KCY4	0.858	3.58	0.729	0.899			
		KCY5	0.819	3.62	0.607	0.872			
Awareness	0.966	ACY1	0.816	4.08	0.579	0.856	88.109		
		ACY2	0.934	4.15	0.674	0.948			
		ACY3	0.895	4.17	0.653	0.923			
		ACY4	0.911	4.08	0.685	0.938			
		ACY5	0.966	4.07	0.690	0.971			
Vulnerabilities	0.978	VCY1	0.936	4.31	0.589	0.948	89.411		
		VCY2	0.923	4.32	0.584	0.939			
		VCY3	0.921	4.32	0.588	0.934			
		VCY4	0.955	4.31	0.581	0.961			
		VCY5	0.939	4.32	0.588	0.950			
		VCY6	0.895	4.33	0.591	0.916			
		VCY7	0.909	4.30	0.597	0.931			
Response	0.967	RCY1	0.900	4.02	0.399	0.925	86.134		
		RCY2	0.918	4.01	0.396	0.940			
		RCY3	0.912	4.03	0.405	0.930			
		RCY4	0.945	4.00	0.369	0.953			
		RCY5	0.845	4.03	0.375	0.879			
		RCY6	0.849	4.06	0.417	0.886			
Impact	0.957	ICY1	0.965	4.09	0.531	0.978	91.668		
		ICY2	0.940	4.09	0.532	0.962			
		ICY3	0.927	4.08	0.539	0.954			
		ICY4	0.924	4.09	0.545	0.950			
		ICY5	0.909	4.09	0.547	0.940			

Notes: [a]Cumulative variance extracted when EFA run for all constructs; [b]KMO measure of sampling adequacy

Table V. Final EFA results of cyberterrorism scale

results of this analysis can be found in Appendix 1. They showed unidimensionality of all constructs, as expected, based on the prior theoretical model. To carry out CFA, the researcher tested each construct each time in AMOS.20 (structural equation modelling software). CFA was used for each construct at a time to ensure a reasonable parameter of estimate-to-observation ratios (Bentler *et al.*, 1987; Jöreskog, 1993). The researcher examined some fit indices which were used, such as chi-square/df (CMIN/df), CFI[1], GFI, AGFI, root mean square error of approximation (RMSEA), standardised RMR (SRMR) and PCLOSE to check the validity of the measurement model (either all or some of them, depending on what was available in the results). Table VI shows the threshold guidelines of GFI used in this study[2].

The results of CFA are presented in Appendix 2. They indicated good unidimensionality with satisfactory fit indices. Therefore, there was no need to delete items. In the following section, there are additional indices and tests (e.g. composite reliability, AVE, convergent and discriminant validity) which are reported by using PLS.

Structural equation modelling using PLS

Using PLS path modelling for assessing hierarchical construct models is a relatively new and rarely used method (Wetzels *et al.*, 2009). "However, several authors have discussed both the theoretical and empirical contributions hierarchical models can make" (Edwards, 2001; Wetzels *et al.*, 2009; Edwards *et al.*, 2000; Burke *et al.*, 2003; Law *et al.*, 1998; MacKenzie *et al.*, 2005; Petter *et al.*, 2007). This study is in line with the previous research (Wetzels *et al.*, 2009), which recommended conducting further studies using PLS path modelling for assessing hierarchical construct models; this study is consistent with it, making it also a contribution to this trend.

Measurement models assessment

Reflective measures

The reflective measurement model is linked to the relationship between the observed variables and latent variables. To evaluate the reflective measurement model, the reliability and validity of the items and constructs of this model were assessed to ensure that only reliable and valid measurements were used before any further assessment of the relationships in the model. Therefore, the models of this study consist of reflective measurements, which should be evaluated with respect to reliability and validity (Bollen, 1998).

Reliability. Cronbach's alpha (Cronbach, 1951) is a common criterion for internal consistency. For the two scales, all constructs showed satisfactory results of Cronbach's alpha, ranging from 0.821 to 0.978 (Tables IV and V). However, while Cronbach's α "tends to provide a severe underestimation of the internal consistency reliability of latent variables in PLS path models" (Henseler *et al.*, 2009, p. 299), it is more appropriate to apply a different measure, the composite reliability (Werts *et al.*, 1974).

The data revealed that all the measures are solid in their internal consistency reliability, as indicated by the composite reliability in Table VII. In all scales, the composite reliabilities of the measures ranged from 0.879 to 0.976, which exceeded the recommended threshold value of 0.8 or 0.9 (Nunnally and Bernstein, 1994).

Given that this study is to verify the validity of the grounded theory, and as a step in the scale development, the reliability of individual items was evaluated by testing loadings of all measures with their perspective factors obtained from PLS (i.e. outer loadings). All items

Chi-square/df (cmin/df)	<3 good; <5 sometimes permissible
p-value for the model	>0.05
CFI	>0.95 great; >0.90 traditional; >0.80 sometimes permissible
GFI	>0.95
AGFI	>0.80
SRMR	<0.09
RMSEA	<0.05 good; 0.05-0.10 moderate; >0.10 bad
PCLOSE	>0.05

Table VI. Goodness of fit thresholds guideline

Constructs	Composite reliability	Cronbach's alpha	AVE
Conventional terrorism (CO)			
Knowledge	0.9356	0.9130	0.7448
Awareness	0.9712	0.9626	0.8712
Vulnerabilities	0.9138	0.8596	0.7796
Response	0.9701	0.9613	0.8664
Impact	0.8797	0.8208	0.6472
Cyberterrorism (CY)			
Knowledge	0.9514	0.9361	0.7971
Awareness	0.9737	0.9659	0.8811
Vulnerabilities	0.9764	0.9702	0.8941
Response	0.9738	0.9676	0.8610
Impact	0.9621	0.9772	0.9167

Table VII. Overview results of the two scales

with loadings greater than 0.7 were retained and therefore considered to be highly reliable. Table VIII shows the factor loadings from the PLS measurement model.

It was noted that all measures loaded remarkably well, as loadings ranged from 0.7547 to 0.9787 on their respective factors in both scales, which is an index of an indicator's reliability (Fornell and Larcker, 1981).

As for the assessment of validity, there are two types of validity always to be evaluated: the convergent validity and the discriminant validity.

Convergent validity. Convergent validity is the extent to which the underlying variable is linked to the pre-defined indicators to measure the same construct (Gerbing and Anderson, 1988). Convergent validity was assessed by the researcher by checking the average variance extracted (AVE) index. Table VII shows that the AVE for all constructs went beyond the minimum threshold value of 0.5, demonstrating that all latent variables explain more than 50 per cent of the variance in their manifest variables (observed variables) (Götz *et al.*, 2010).

Discriminant validity. Discriminant validity is the extent to which the indicators of one construct are distinct from the items of other latent variables (Bagozzi *et al.*, 1991). In this study, as it uses PLS, discriminant validity can be assessed using two criteria. The first of these is the Fornell-Larcker criterion which is on the construct level. It is measured by computing the AVE for each construct and comparing it with the square correlation between all constructs, and if the AVE estimates exceed the squared correlation estimates for any of the constructs, then the discriminant validity is attained (Fornell and Larcker, 1981). Table IX shows that the root AVE values, in all cases, are greater than the corresponding off-diagonal correlations, pointing to sufficient discriminant validity.

The second criterion used is cross-loadings, which are on the indicator level, as the loading of each indicator is supposed to be greater than all of its cross-loadings, providing a further check for discriminant validity (Götz *et al.*, 2010; Chin, 1998). Table X illustrates the results of this study.

To summarise, based on all previous evaluations, (i.e. reliability, convergent validity and discriminant validity) in each of the two scales, all measurement items showed satisfactory reliability and validity, so they were all retained.

Items	Knowledge	Awareness	Vulnerabilities	Response	Impact
Conventional terrorism (CO)					
KCO1	0.7623				
KCO2	0.8507				
KCO3	0.9365				
KCO4	0.8904				
KCO5	0.8656				
ACO1		0.8704			
ACO2		0.9545			
ACO3		0.9281			
ACO4		0.9376			
ACO5		0.9730			
VCO1			0.8516		
VCO2			0.9269		
VCO3			0.8687		
RCO1				0.9222	
RCO2				0.9516	
RCO3				0.9634	
RCO4				0.9024	
RCO5				0.9131	
ICO1					0.7739
ICO2					0.8146
ICO3					0.8699
ICO4					0.7547
Cyberterrorism (CO)					
KCY1	0.9207				
KCY2	0.8081				
KCY3	0.9451				
KCY4	0.9059				
KCY5	0.8780				
ACY1		0.8798			
ACY2		0.9603			
ACY3		0.9299			
ACY4		0.9415			
ACY5		0.9787			
VCY1			0.9544		
VCY2			0.9454		
VCY3			0.9438		
VCY4			0.9674		
VCY5			0.9540		
VCY6			0.9208		
VCY7			0.9324		
RCY1				0.9261	
RCY2				0.9400	
RCY3				0.9423	
RCY4				0.9645	
RCY5				0.8927	
RCY6				0.8997	
ICY1					0.9783
ICY2					0.9620
ICY3					0.9539
ICY4					0.9510
ICY5					0.9416

Table VIII.
Factor loadings for the two scales

Constructs	Knowledge	Awareness	Vulnerabilities	Response	Impact
Conventional terrorism (CO)					
Knowledge	**0.8630**				
Awareness	*0.0408*	**0.9334**			
Vulnerabilities	*−0.2896*	*0.0304*	**0.8829**		
Response	*0.0080*	*−0.2732*	*0.0214*	**0.9308**	
Impact	*−0.0422*	*0.0499*	*0.0571*	*−0.0319*	**0.8045**
Cyberterrorism (CY)					
Knowledge	**0.8928**				
Awareness	*0.0062*	**0.9387**			
Vulnerabilities	*−0.1946*	*0.0865*	**0.9456**		
Response	*0.0292*	*−0.2710*	*−0.0983*	**0.9279**	
Impact	*−0.0501*	*−0.0220*	*−0.0117*	*0.0072*	**0.9574**

Note: The bold values are the root AVE values, in all cases, are greater than the corresponding off-diagonal correlations, pointing to sufficient discriminant validity

Table IX. Latent variable correlations

Formative measure

In formative measurement, traditional assessment theory and the classical validity test are not applicable to variables that are used in formative measurement models (Bollen, 1998). Because this study uses latent variables (i.e. knowledge, awareness […]) as a second-order formative measurement model in hierarchical construct models, the concepts of reliability (i.e. internal consistency) and construct validity (i.e. convergent and discriminant validity) are not feasible as formative measures.

For this reason, the second-order formative construct was interpreted based on weights instead of loadings (Petter *et al.*, 2007; Wetzels *et al.*, 2009) Figure 5 shows the PLS results and Table XI shows the weights of formative constructs for conventional terrorism.

Figure 6 shows the PLS results and Table XI shows the weights of formative constructs for cyberterrorism.

As the formative measurement model is based on multiple regression, multicollinearity could pose a relevant problem in formative constructs (Diamantopoulos and Winklhofer, 2001). However, in this study, all values for the variance inflation factor were very acceptable ranging from 1.004 to 1.105 for both scales. As the common cut-off threshold is 10 (Kleinbaum *et al.*, 2013; Sarstedt and Ringle, 2010), the previous results are very reassuring, as there was no multicollinearity.

Redundancy analysis is the first step in assessing the formative measurement's convergent validity before *t*-statistics. The test is run by correlating the formatively measured construct with a reflective measure of the same construct. A value above 0.8, ideally 0.9, is considered to be valid (Hair, 2014). As shown in Figures 7 and 8, the results for the redundancy analysis for the conventional threat and cyber threat constructs yield a path coefficient of 0.954 and 0.975, respectively, which are robust and above the threshold of 0.9, thus providing support for the formative constructs' convergent validity.

Structural model assessment

The structural model aims to specify relations between latent constructs in different orders. The structural model testing was carried out after the two scales of validity and reliability

Items	Knowledge	Awareness	Vulnerabilities	Response	Impact
Conventional terrorism (CO)					
KCO1	**0.7623**	0.1293	−0.1524	−0.0746	0.0674
KCO2	**0.8507**	0.0700	−0.2959	−0.0449	−0.0688
KCO3	**0.9365**	−0.0002	−0.2533	0.0145	0.0006
KCO4	**0.8904**	−0.0598	−0.3182	0.0942	−0.1107
KCO5	**0.8656**	0.0262	−0.2434	0.0540	−0.0892
ACO1	0.0272	**0.8704**	0.0851	−0.2774	0.0418
ACO2	0.0508	**0.9545**	0.0258	−0.2569	0.0591
ACO3	0.0327	**0.9281**	0.0210	−0.2541	0.0399
ACO4	0.0228	**0.9376**	0.0127	−0.2354	0.0344
ACO5	0.0546	**0.9730**	0.0027	−0.2541	0.0561
VCO1	−0.2022	0.0959	**0.8516**	−0.1010	0.1073
VCO2	−0.3041	−0.0524	**0.9269**	0.1161	0.0426
VCO3	−0.2728	0.0157	**0.8687**	0.0750	−0.0129
RCO1	−0.0473	−0.2441	0.0317	**0.9222**	−0.0368
RCO2	0.0018	−0.2550	0.0161	**0.9516**	−0.0731
RCO3	0.0040	−0.2743	0.0264	**0.9634**	0.0030
RCO4	0.0739	−0.2687	−0.0143	**0.9024**	−0.0133
RCO5	−0.0049	−0.2275	0.0408	**0.9131**	−0.0338
ICO1	−0.0526	−0.0139	−0.0242	−0.0083	**0.7739**
ICO2	0.0362	0.0774	0.1634	−0.0540	**0.8146**
ICO3	−0.0280	0.0021	−0.0288	0.0088	**0.8699**
ICO4	−0.1335	0.0812	0.0217	−0.0405	**0.7547**
Cyberterrorism (CO)					
KCY1	**0.9207**	0.0027	−0.1351	0.0211	−0.0407
KCY2	**0.8081**	0.0725	−0.2351	−0.0496	−0.0644
KCY3	**0.9451**	−0.0078	−0.0946	0.0193	−0.0221
KCY4	**0.9059**	−0.0565	−0.2455	0.0875	−0.0614
KCY5	**0.8780**	0.0286	−0.2155	0.0466	−0.0500
ACY1	0.0117	**0.8798**	0.1281	−0.2782	−0.0304
ACY2	0.0197	**0.9603**	0.0847	−0.2609	−0.0211
ACY3	−0.0019	**0.9299**	0.0768	−0.2498	−0.0274
ACY4	−0.0151	**0.9415**	0.0586	−0.2331	−0.0229
ACY5	0.0131	**0.9787**	0.0593	−0.2502	−0.0028
VCY1	−0.1802	0.0902	**0.9544**	−0.0938	−0.0061
VCY2	−0.1586	0.1126	**0.9454**	−0.1013	−0.0232
VCY3	−0.1908	0.1187	**0.9438**	−0.1099	−0.0070
VCY4	−0.1947	0.0888	**0.9674**	−0.0840	0.0008
VCY5	−0.1925	0.0511	**0.9540**	−0.0950	−0.0268
VCY6	−0.1887	0.0586	**0.9208**	−0.1151	0.0080
VCY7	−0.1841	0.0470	**0.9324**	−0.0519	−0.0236
RCY1	−0.0163	−0.2448	−0.1096	**0.9261**	0.0138
RCY2	−0.0109	−0.2357	−0.0987	**0.9400**	0.0052
RCY3	0.0342	−0.2547	−0.0794	**0.9423**	−0.0255
RCY4	0.0309	−0.2744	−0.0805	**0.9645**	0.0326
RCY5	0.0812	−0.2667	−0.1026	**0.8927**	−0.0033
RCY6	0.0355	−0.2302	−0.0823	**0.8997**	0.0144
ICY1	−0.0466	−0.0112	−0.0063	−0.0076	**0.9783**
ICY2	−0.0546	−0.0073	−0.0227	−0.0054	**0.9620**
ICY3	−0.0334	−0.0053	−0.0248	−0.0061	**0.9539**
ICY4	−0.0457	−0.0308	−0.0099	0.0207	**0.9510**
ICY5	−0.0598	−0.0513	0.0075	0.0338	**0.9416**

Note: As the bold values are cross-loadings, which are on the indicator level, as the loading of each indicator is greater than all of its cross-loadings, providing a further check for discriminant validity

Table X.
Cross-loadings for both scales

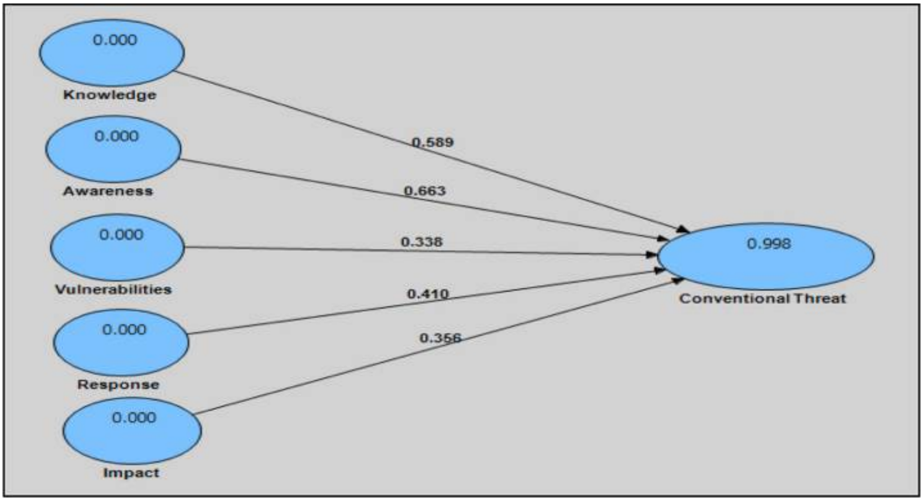

Figure 5. PLS results for weights of conventional threat formative construct

Table XI. Outer weights and collinearity statistics of formative latent variables

Formative construct	Weights	Collinearity statistics Tolerance	VIF[a]
Conventional terrorism			
Knowledge → Threat	0.5893***	0.905	1.105
Awareness → Threat	0.6634***	0.922	1.085
Vulnerabilities → Threat	0.3377***	0.906	1.103
Response → Threat	0.4099***	0.923	1.084
Impact → Threat	0.3558***	0.994	1.006
Cyberterrorism			
Knowledge → Threat	0.4962***	0.956	1.047
Awareness → Threat	0.5117***	0.923	1.083
Vulnerabilities → Threat	0.6417***	0.946	1.057
Response → Threat	0.3649***	0.922	1.085
Impact → Threat	0.4271***	0.996	1.004

Note: [a] VIF = (1/tolerance)

were achieved. They are tested by estimating the paths between the first-order reflective constructs, and the second-order formative constructs, in a hierarchical latent variable model, which is an indicator of the model's predictive ability. To assess the structural model, the coefficient parameter estimates were tested, as well as the GFIs (Appendix 2) to assess if the hypothesised structural model fits the data. So, the hypothesised model was tested and the results are presented in Table XII, which indicates that all the hypotheses are accepted. Further details are discussed in the following section.

Results of testing the hypotheses

Cyberterrorism

Knowledge of cyberterrorism and the threat. As shown earlier, *HA1* explained the relationship between the knowledge of cyberterrorism and the total threat. As outlined

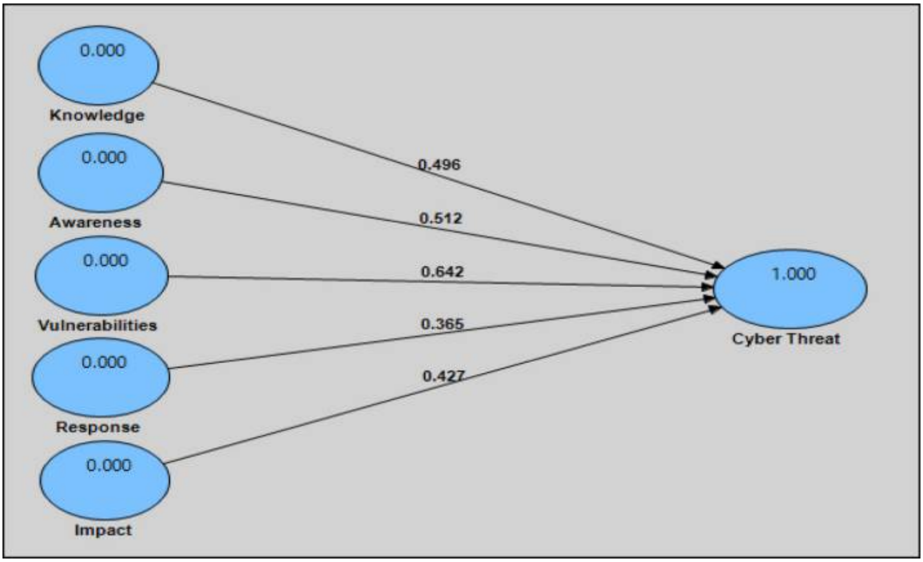

Figure 6.
The PLS results for weights of cyber threat formative construct

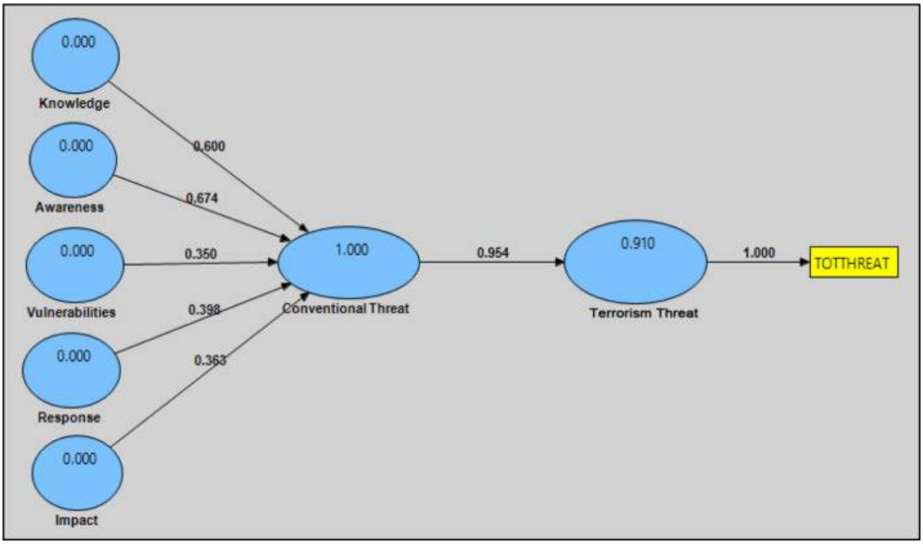

Figure 7.
Redundancy analysis result for conventional threat model

in Table XII, the hypothesised relationship was found to be significant (ß = 0.496, *t*-value = 10.9). Thus, this hypothesis was supported.

Awareness of cyberterrorism and the threat. *HA2* represented the relationship between the awareness of cyberterrorism and the total threat; *HA2* was supported as the parameter estimates were significant (ß = 0.512, *t*-value = 12.1) (Table XII).

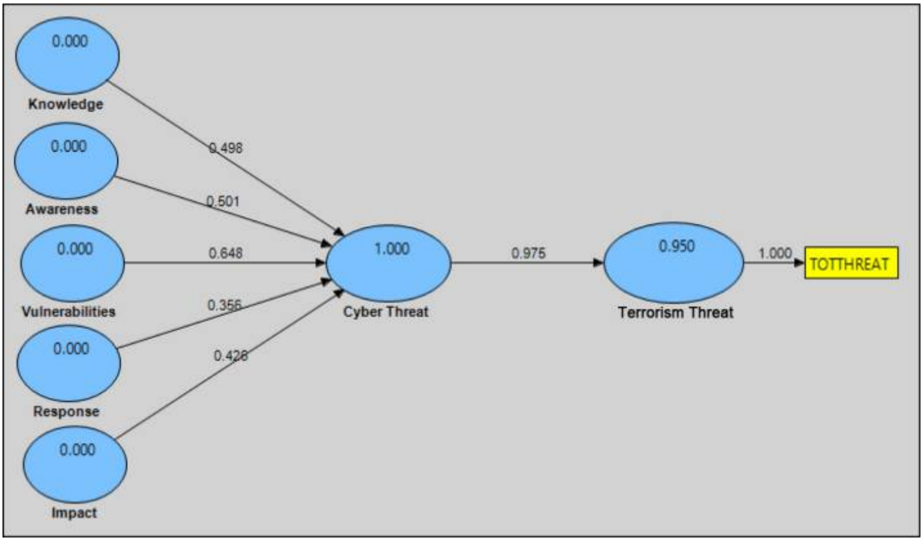

Figure 8.
Redundancy analysis result for cyber threat model

Vulnerabilities of cyberterrorism and the threat. *HA3* is the relationship between vulnerabilities of cyberterrorism and the total threat; results showed a significant path (ß = 0.642, *t*-value = 11.2), and thereby *HA3* was supported (Table XII).

Response to cyberterrorism and the threat. The relationship between the response to cyberterrorism and the total threat is explained by *HA4*; results in Table XII indicate that this hypothesis is statistically significant (ß = 0.365, *t*-value = 6.1). Thus, this hypothesis was supported.

Impact of cyberterrorism and the threat. According to Table XII, the hypothesis explaining the relationship between the impact of cyberterrorism and the total threat, *HA5*, was supported because it was found significant in the hypothesised direction (ß = 0.427, *t*-value = 10.7).

As a result of the support and acceptance of all previous hypotheses without any exception as shown above, the main *HA* that the conceptual framework (Grounded theory) for cyberterrorism will be statistically valid, is thus accepted and supported (Table XII and Figure 9).

Conventional terrorism

Knowledge of conventional terrorism and the threat. *HB1*, which explains the relationship between the knowledge of conventional terrorism and the total threat, was supported as the parameter estimate was significant (ß = 0.589, *t*-value = 12.9) (see Table XII).

Awareness of conventional terrorism and the threat. According to Table XII, the hypothesis explaining the relationship between the awareness of conventional terrorism and the total threat, *HB2*, was supported as the results showed a significant path (ß = 0.663, *t*-value = 15.7).

Vulnerabilities of conventional terrorism and the threat. *HB3* which represents the relationship between the vulnerabilities of conventional terrorism and the total threat was found statistically significant (ß = 0.338, *t*-value = 6.6), and thus supported (Table XII).

	Hypotheses	Path estimates	Standard error	t-value	Test results
Cyberterrorism (CY)					
H_{A1}	Knowledge of cyberterrorism will be highly related to identifying and assessing the threat	0.4962***	0.0455	10.8972	Accepted
H_{A2}	Awareness of cyberterrorism will be highly related to identifying and assessing the threat	0.5117***	0.0423	12.1026	Accepted
H_{A3}	Vulnerabilities of cyberterrorism will be highly related to identifying and assessing the threat	0.6417***	0.0572	11.2155	Accepted
H_{A4}	Response to cyberterrorism will be highly related to identifying and assessing the threat	0.3649***	0.0598	6.1059	Accepted
H_{A5}	Impact of cyberterrorism will be highly related to identifying and assessing the threat	0.4271***	0.0401	10.6553	Accepted
Conventional terrorism (CO)					
H_{B1}	Knowledge of conventional terrorism will be highly related to identifying and assessing the threat	0.5893***	0.0456	12.9322	Accepted
H_{B2}	Awareness of conventional terrorism will be highly related to identifying and assessing the threat	0.6634***	0.0423	15.6998	Accepted
H_{B3}	Vulnerabilities of conventional terrorism will be highly related to identifying and assessing the threat	0.3377***	0.0514	6.5644	Accepted
H_{B4}	Response to conventional terrorism will be highly related to identifying and assessing the threat	0.4099***	0.0607	6.7557	Accepted
H_{B5}	Impact of conventional terrorism will be highly related to identifying and assessing the threat	0.3558***	0.0316	11.2616	Accepted

Note: $p < 0.001$

Table XII.
Results of testing the hypotheses

Response to conventional terrorism and the threat. According to Table XII, the hypothesis explaining the relationship between response of conventional terrorism and the total threat, *HB4*, was supported because it was found significant in the hypothesised direction (ß = 0.410, t-value = 6.8).

Impact of conventional terrorism and the threat. As shown in Table XII, *HB5*, which explains the relationships between impact of conventional terrorism and the total threat, was supported as the hypothesised relationship was found to be significant (ß = 0.336, t-value = 11.3).

As a result of the support and acceptance of all previous hypotheses without any exception as shown above, the main *HB* that the conceptual framework (Grounded theory) for conventional terrorism will be statistically valid, is thus accepted and supported (Table XII and Figure 10).

Figures 9 and 10 summarise the results obtained for each hypothesised path in the two models, indicating the overall acceptability of the structural model analysed.

In the hierarchical model, there is aggregation between the threat of cyber and conventional terrorism statistically in the third formative order construct (Total Threat). The two types of threat can be aggregated in one construct, as they have high path estimates and they are all statistically significant, as for cyberterrorism threat

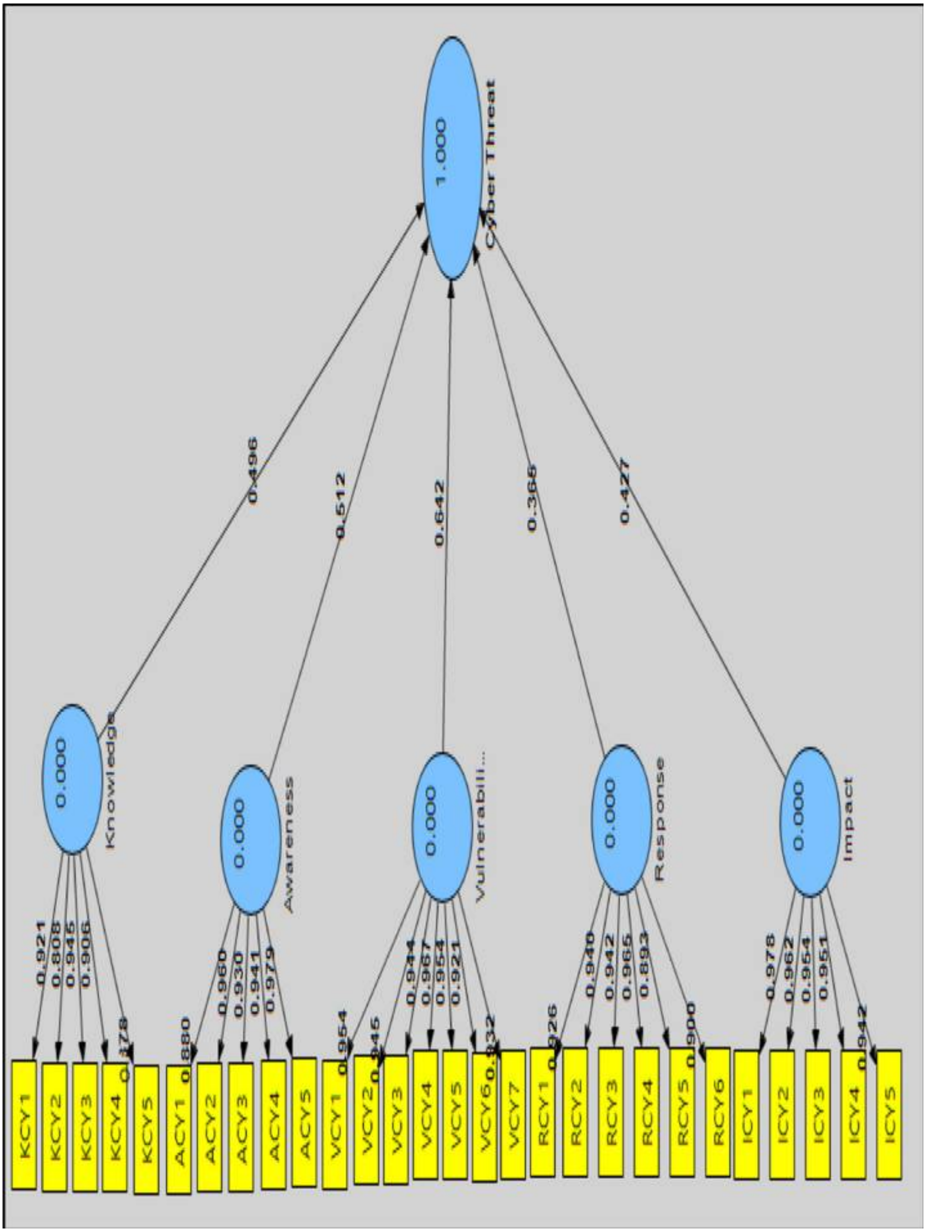

Figure 9.
Validated structural model of cyberterrorism threat

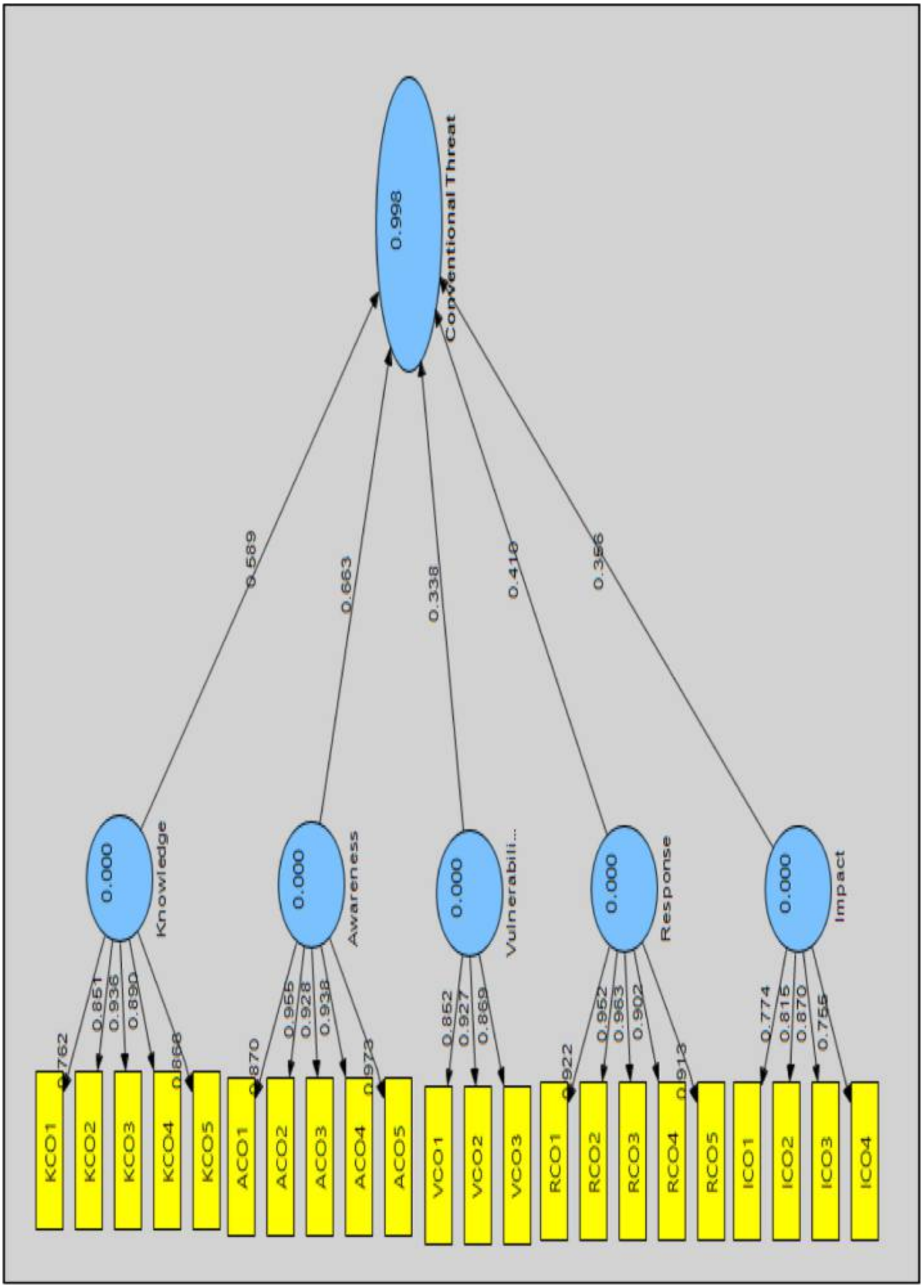

Figure 10.
Validated structural model of conventional terrorism threat

(ß = 0.594, *t*-value = 46.7) and for conventional terrorism threat (ß = 0.442, *t*-value = 32.2), as shown in Table XIII. This confirms and supports the fact that both models are valid and reliable and can be applied to each of the two threats, as they can be aggregated with each other to identify the total threat (Figure 11). The full model can be found in Appendix 3.

For the goodness-of-fit evaluation, the GFI is defined as the geometric mean of the average communality and average R^2 for all constructs (Tenenhaus *et al.*, 2005). It can be applied to define the overall prediction power of a large complex model by accounting for the performance of both measurement and structural parameters (Akter *et al.*, 2011). The GFI is crucial to assess the global validity of a PLS-based complex model (Tenenhaus *et al.*, 2005). According to Chin (2010), "The intent is to account for the PLS model performance at both the measurement and the structural model with a focus on overall prediction performance of the model"). The GFI is applied for both reflective and formative latent variables in a complex case, as it provides a measure of overall fit (Vinzi *et al.*, 2005; Chin, 2010). The GFI is bounded between 0 and 1 (Vinzi *et al.*, 2005; Chin, 2010). For the model depicted in Figure 11, this study obtains a GFI value of 0.930 as shown in Table XIV. This finding indicates that the model has a robust prediction power and adequately validates this complex model.

Summary and conclusion

The aim of this paper (quantitative) is to examine the validity of the grounded theory resulting from a previous phase (qualitative). The conceptual framework and the

Formative construct	Total terrorism threat Path estimates	Standard error	*t*- value
Cyberterrorism → terrorism threat	0.5937***	0.0127	46.7027
Conventional terrorism → terrorism threat	0.4416***	0.0137	32.1536

Note: $p < 0.001$

Table XIII. Results of testing the third formative latent constructs

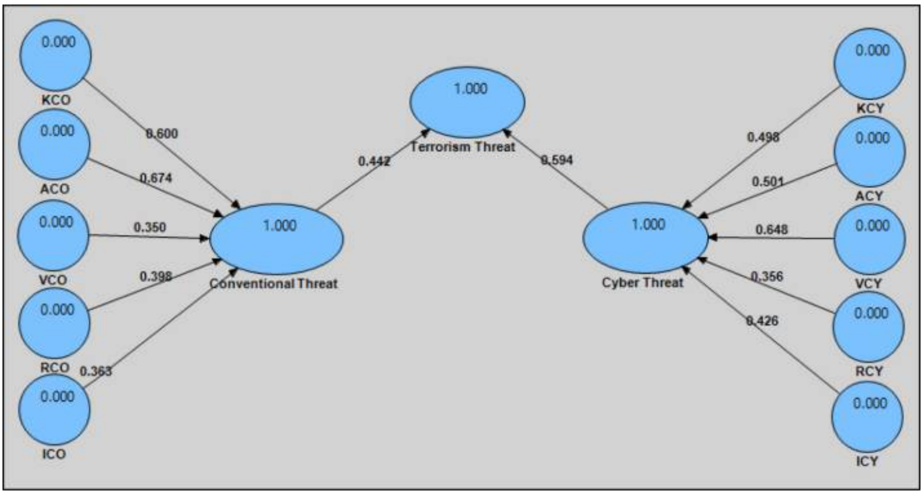

Figure 11. Validated structural model of cyber and conventional terrorism threat

Table XIV.
GFI results

Block	Conventional terrorism (CO) R^2	Communality
COTH	0.9977	1.0000
CYTH	0.9997	1.0000
TOTTH	1.0000	1.0000
KCO		0.7448
KCY		0.7971
ACO		0.8712
ACY		0.8811
VCO		0.7796
VCY		0.8941
RCO		0.8664
RCY		0.8610
ICO		0.6472
ICY		0.9167
Average	**0.9991**	**0.8661**
GoF[a]	**0.930**	

Note: [a] GoF average R^2 average communality, which is 0.930 in this case. This finding indicates that the model has a robust prediction power and adequately validates this complex model
Source: Tenenhaus *et al.* (2005)

hypotheses of this phase were developed based on the developed grounded theory. The model consists of five first order reflective constructs, which are knowledge, awareness, vulnerabilities, response and impact. These constructs represent 22 measurement items in the conventional terrorism threat model and 28 items in the cyberterrorism model. These two models have second and third formative constructs and they can be aggregated in one final model.

This paper reported the results of the data analysis for the quantitative phase of this study. First, it showed the results of the pilot study and the items that were excluded from the instrument. Then, the demographic characteristics of this sample were described, followed by conducting a reliability test and EFA then CFA.

In the second part of the analysis, SEM was conducted in two stages, the measurement model and the structural model. In the first stage, the fit of the measurement model was assessed. The results showed that all indicators were highly loaded on their specified factors and each construct was then tested for reliability and validity. The overall GFIs suggested acceptance of the models. In the next stage, the structural model was assessed and the results showed a good fit of the models to the data. All pathways are significant and all the hypotheses were supported. Consequently, the two models provide a robust test of the hypothesised relationships between the constructs indicating valid and reliable models.

The several theoretical contributions provided by this study can be summarised in the following points: first, this research study contributes to the literature of terrorism in general, and in particular to the literature of cyberterrorism, by providing a theoretical framework for potential terrorist threats, whether conventional or cyber, to national security. This theoretical framework draws a holistic picture of the underlying aspects of the terrorist threats to promote a clear understanding of the aspects of this imminent phenomenon. What distinguishes this theoretical framework is that it is built on empirical data collected from critical infrastructure sectors in Saudi Arabia as a dynamic state in the Middle East. This case study represents the countries of the region and can be applied anywhere else.

Second, this theoretical framework contributes to the attempt to unify the understanding and perception of the different levels of researchers, technicians, military and security officials, and decision makers. It is obvious that the perception of these terrorist threats varies from one person to another at different levels. So this theoretical framework describes clear milestones of the phenomenon which can be understood at all different levels. At the same time, this theoretical model lays the foundation for the understanding and perception of different potential security threats, so that it can be applied in different contexts, provided it continues to be developed and updated to correspond to the emerging threats.

Third, this study provides an integrative perception of cyberterrorism and conventional terrorism simultaneously. Comparison between these different terrorist threats shows similarities and differences through consultation with the proposed theoretical framework. This study clearly shows the comparative approach between the two phenomena involved in many of the characteristics and dimensions. However, one is more familiar to the research society (conventional terrorism) and the other is relatively new (cyberterrorism). This approach is appropriate and effective for exploratory studies of emerging security threats by linking them to previous familiar threats, which facilitates understanding, detection and control measures.

Fourth, this study also advances the debate about the reality of cyberterrorism, and how realistic it is that there will be terrorist cyber threats to national security. The research provides evidence built on empirical data, proving that the terrorist cyber threats are real and realistic, and critical infrastructure may be exposed to them in any place and at any time. As terrorism itself is a social phenomenon related to society, it is affected by changes that occur in society. As technological progress is one of the most important transformations in the twenty-first century, terrorism is not, and will not, stay with arms folded towards the exploitation of this technology to launch their attacks and to promote their propaganda. Hence, governments and people should prepare for such threats in various ways, thus avoiding a new cyber-Pearl Harbour. To this end, through the application of the aspects of the proposed theoretical framework, it contributes to the identification and evaluation of potential security threats in general, and cyber-terrorist threats in particular, in a practical and systematic way. Furthermore, due to the nature of the interdependence between critical infrastructure sectors, the managers and technicians and officials should be aware of this when developing their response. This response, as the study showed, revolves around four themes: interdiction, prevention, detection and reaction. Consequently, one of the contributions of this study is to provide a foundation for a road map to officials in the infrastructure sectors to control terrorist threats, whether they be cyber or conventional, legally and practically. It is incumbent upon those officials to develop and modify it according to their own infrastructure sector. An overview of how to implement the proposed theoretical framework will be a direction for future research. The researcher is now working on a proposed strategy based on this framework.

Fifth, this study contributes to raising the level of knowledge and awareness of cyber terrorist threats among officials and employees in critical infrastructure. Knowledge and awareness are directly correlated; the more knowledge exists about terrorist threats, the greater the awareness of these threats. From this perspective, education, educational courses and cognitive capabilities of the staff are important means to raise awareness of the threats and thus lower the level of risk. Adequate and moderate awareness acts as a catalyst for vigilance and the search for sources of threats and vulnerabilities that may be exploited. The awareness of the threats among managers and officials will lead to educating employees about these threats and to taking all the precaution measures necessary to combat these threats. These two factors are the baseline of this theoretical framework, as knowledge and awareness are the first footsteps in the fight against cyberterrorism. This matter should be given utmost attention by the administrators, military and security officials, technicians and executives, in critical infrastructure sectors.

Sixth, with regard to methodology, the major contribution of this study is that it is the first of its kind – to the knowledge of the researcher – to use mixed method focusing on grounded theory to develop a theoretical framework for the potential terrorist threats to national security, and to test its validity statistically in the same study. Interviews enabled the researcher to explore the concept of the potential threat of cyberterrorism to Saudi national security, which had not previously been examined, and to develop the research's theoretical framework. Then, the quantitative phase followed, with a survey analysed through SEM PLS. This specific combined approach (interviews and SEM PLS) has not commonly been used in this area of research. Hence, such an attempt should set a new benchmark for future research carried out in this field.

Succinctly, this research is the first that aims to develop a theoretical framework for the potential threats of cyberterrorism to Saudi national security, compared with the more familiar conventional terrorism. In bringing together empirical data and a previous qualitative study with the current quantitative one, this study provides important theoretical contributions and implications to the cyberterrorism field, and to employees and managers in the critical infrastructure as well as to decision-makers, all of which support the stability of national security.

Notes

1. CFI (comparative fit Index), GFI (goodness of fit index), AGFI (adjusted goodness of fit index).
2. Adopted by Gaskin http://statwiki.kolobkreations.com from, Hair *et al.* (2010, p. 654).

References

Akter, S., D'Ambra, J. and Ray, P. (2011), "An evaluation of PLS based complex models: the roles of power analysis, predictive relevance and GOF index", *Proceedings of the Seventeenth Americas Conference on Information Systems*, *Detroit, MI*, 4-7 August.

Anderson, J.C. and Gerbing, D.W. (1982), "Some methods for respecifying measurement models to obtain unidimensional construct measurement", *Journal of Marketing Research*, Vol. 19 No. 4, pp. 453-460.

Anderson, J.C., Gerbing, D.W. and Hunter, J.E. (1987), "On the assessment of unidimensional measurement: internal and external consistency, and overall consistency criteria", *Journal of Marketing Research*, Vol. 24 No. 4, pp. 432-437.

Bagozzi, R.P., Yi, Y. and Phillips, L.W. (1991), "Assessing construct validity in organizational research", *Administrative Science Quarterly*, Vol. 36 No. 3, pp. 421-458.

Bartlett, M.S. (1954), "A note on the multiplying factors for various X 2 approximations", *Journal of the Royal Statistical Society. Series B (Methodological)*, Vol. 16 No. 2, pp. 296-298.

Bentler, P.M. and Chou, C.-P. (1987), "Practical issues in structural modeling", *Sociological Methods & Research*, Vol. 16 No. 1, pp. 78-117.

Bollen, K.A. (1998), *Structural Equation Models*, Wiley Online Library, Hoboken, NJ.

Burke, J.C., MacKenzie, S.B. and Podsakoff, P.M. (2003), "A critical review of construct indicators and measurement model misspecification in marketing and consumer research", *Journal of Consumer Research*, Vol. 30 No. 3, pp. 199-218.

Child, D. (1990), *The Essentials of Factor Analysis (2nd ed.)*, Cassell Educational, New York, NY.

Chin, W.W. (1998), "The partial least squares approach to structural equation modeling", *Modern Methods for Business Research*, Vol. 295 No. 2, pp. 295-336.

Chin, W.W. (2010), "How to write up and report PLS analyses", *Handbook of Partial Least Squares*, Springer, Berlin, Heidelberg, pp. 655-690.

Churchill, G.A. Jr (1979), "A paradigm for developing better measures of marketing constructs", *Journal of Marketing Research*, Vol. 16 No. 1, pp. 64-73.

Collin, B. (2013), "The future of cyberterrorism: where the physical and virtual worlds converge", 11th Annual International Symposium on Criminal Justice Issue, Institute for Security and Intelligence, available at: http://afgen.com/terrorism1.html (accessed 16 June 2013).

Cronbach, L.J. (1951), "Coefficient alpha and the internal structure of tests", *Psychometrika*, Vol. 16 No. 3, pp. 297-334.

Diamantopoulos, A. and Winklhofer, H.M. (2001), "Index construction with formative indicators: an alternative to scale development", *Journal of Marketing Research*, Vol. 38 No. 2, pp. 269-277.

Edwards, J.R. (2001), "Multidimensional constructs in organizational behavior research: an integrative analytical framework", *Organizational Research Methods*, Vol. 4 No. 2, pp. 144-192.

Edwards, J.R. and Bagozzi, R.P. (2000), "On the nature and direction of relationships between constructs and measures", *Psychological Methods*, Vol. 5 No. 2, pp. 155-174.

Field, A. (2013), *Discovering Statistics Using IBM SPSS Statistics*, Sage, London.

Fornell, C. and Larcker, D.F. (1981), "Structural equation models with unobservable variables and measurement error: algebra and statistics", *Journal of Marketing Research*, Vol. 18 No. 3, pp. 328-388.

Gerbing, D.W. and Anderson, J.C. (1988), "An updated paradigm for scale development incorporating unidimensionality and its assessment", *Journal of Marketing Research*, Vol. 25 No. 2, pp. 186-192.

Götz, O., Liehr-Gobbers, K. and Krafft, M. (2010), "Evaluation of structural equation models using the partial least squares (PLS) approach", *Handbook of Partial Least Squares*, Springer, Berlin, Heidelberg, pp. 691-711.

Hair, J.F. (2010), *Multivariate Data Analysis*, 7th ed., Prentice Hall, Upper Saddle River, NJ.

Hair, J.F. (2014), *A Primer on Partial Least Squares Structural Equations Modeling (PLS-SEM)*, SAGE, Los Angeles, CA.

Hair, J.F., Tatham, R.L., Anderson, R.E. and Black, W. (2006), *Multivariate Data Analysis*, 5th ed., Pearson, Prentice Hall Upper Saddle River, NJ.

Henseler, J., Ringle, C.M. and Sinkovics, R.R. (2009), "The use of partial least squares path modeling in international marketing", *Advances in International Marketing*, Vol. 20 No. 1, pp. 277-319.

Inoguchi, T. (1996) *Our Planet and Human Security*, United Nations University, Kobe, available at: www.unu.edu/unupress/planet.html#Preface (accessed 8 June 2013).

Jöreskog, K.G. (1993), in Bollen, K.A. and Long, J.S. (Eds), *Testing Structural Equation Models*, SAGE Publications, Newbury Park, CA, Vol. 154, pp. 294-316.

Kaiser, H.F. and Rice, J. (1974), "Little Jiffy, Mark Iv", *Educational and Psychological Measurement*, Vol. 34 No. 1, pp. 111-117.

Kleinbaum, D., Kupper, L., Nizam, A. and Rosenberg, E. (2013), *Applied Regression Analysis and Other Multivariable Methods*, Cengage Learning, Boston, MA.

Law, K.S., Wong, C.-S. and Mobley, W.M. (1998), "Toward a taxonomy of multidimensional constructs", *Academy of Management Review*, Vol. 23 No. 4, pp. 741-755.

Leech, L.N., Barrett, C.K. and Morgan, A.G. (2008), *Spss for Intermediate Statistics: Use and Interpretation*, 3rd ed., Taylor & Francis Group, LLC, Mahwah, New Jersey.

MacKenzie, S.B., Podsakoff, P.M. and Jarvis, C.B. (2005), "The problem of measurement model misspecification in behavioral and organizational research and some recommended solutions", *Journal of Applied Psychology*, Vol. 90 No. 4, pp. 710-730.

Mythen, G. and Walklate, S. (2006), "Criminology and terrorism: which thesis? Risk society or governmentality?", *The British Journal of Criminology*, Vol. 46, pp. 379-398, available at: http://bjc.oxfordjournals.org/content/46/3/379.abstract (accessed 7 June 2014).

Netemeyer, R.G., Bearden, W.O. and Sharma, S. (2003), *Scaling Procedures: Issues and Applications*, Sage, London, New Delhi.

Nunnally, J. (1978), *Psychometric Theory*, McGraw-Hill, New York, NY.

Nunnally, J.C. and Bernstein, I.H. (1994), *Psychometric Theory*, 3rd ed., McGraw-Hill, New York, NY.

Pallant, J. (2010), *Spss Survival Manual: A Step by Step Guide to Data Analysis Using Spss*, McGraw-Hill International, New York, NY.

Petter, S., Straub, D. and Rai, A. (2007), "Specifying formative constructs in information systems research", *MIS Quarterly*, Vol. 31 No. 4, pp. 623-656.

Rowe, A.J., Davis, S.A. and Vij, S. (1996), *Intelligent Information Systems: Meeting the Challenge of the Knowledge Era*, Quorum, Westport, CT, London.

Sarstedt, M. and Ringle, C.M. (2010), "Treating unobserved heterogeneity in PLS path modeling: a comparison of fimix-PLS with different data analysis strategies", *Journal of Applied Statistics*, Vol. 37 No. 8, pp. 1299-1318.

Schmid, A.P. (2011), *The Routledge Handbook of Terrorism Research*, Routledge, London.

Tabachnick, B.G. and Fidell, L.S. (2007), "Multivariate analysis of variance and covariance", *Using Multivariate Statistics*, Vol. 3, pp. 402-407.

Tadjbakhsh, S. and Chenoy, A. (2007), *Human Security, Concepts and Implications*, Routledge, London, p. 1.

Tenenhaus, M., Vinzi, V.E., Chatelin, Y.-M. and Lauro, C. (2005), "PLS path modeling", *Computational Statistics & Data Analysis*, Vol. 48 No. 1, pp. 159-205.

Vinzi, V.E., Trinchera, L. and Amato, S. (2010), "PLS path modeling: from foundations to recent developments and open issues for model assessment and improvement", *Handbook of Partial Least Squares*, Springer, Berlin, Heidelberg, pp. 47-82.

Werts, C.E., Linn, R.L. and Jöreskog, K.G. (1974), "Intraclass reliability estimates: testing structural assumptions", *Educational and Psychological Measurement*, Vol. 34 No. 1, pp. 25-33.

Wetzels, M., Odekerken-Schroder, G. and van Oppen, C. (2009), "Using PLS path modeling for assessing hierarchical construct models: guidelines and empirical illustration", *Management Information Systems Quarterly*, Vol. 33 No. 1, p. 11.

Appendix 1. Factorability and CFA using SPSS.20

Conventional terrorism
Knowledge

Table AI. KMO and Bartlett's test

KMO measure of sampling adequacy	0.837
Bartlett's Test of Sphericity	
Approximate chi-square	2,124.121
df	10
Significance	0.000

Table AII. Component matrix[a]

	Component 1
KCO1	0.735
KCO2	0.850
KCO3	0.939
KCO4	0.904
KCO5	0.876

Notes: Extraction method: principal component analysis; [a] 1 components extracted

Awareness

Table AIII. KMO and Bartlett's test

KMO measure of sampling adequacy	0.858
Bartlett's Test of Sphericity	
Approximate chi-square	3,474.994
df	10
Significance	0.000

Table AIV. Component matrix[a]

	Component 1
ACO1	0.870
ACO2	0.954
ACO3	0.929
ACO4	0.938
ACO5	0.973

Notes: Extraction method: principal component analysis; [a] 1 components extracted

Vulnerabilities

Table AV.
KMO and Bartlett's test

KMO measure of sampling adequacy	0.733
Bartlett's Test of sphericity	
Approximate chi-square	898.333
df	3
Significance	0.000

Table AVI.
Component matrix[a]

	Component 1
VCO1	0.809
VCO2	0.946
VCO3	0.895

Notes: Extraction method: principal component analysis; [a] 1 components extracted

Response

Table AVII.
KMO and Bartlett's test

KMO measure of sampling adequacy	0.851
Bartlett's Test of Sphericity	
Approximate chi-square	3,461.100
df	10
Significance	0.000

Table AVIII.
Component matrix[a]

	Component 1
RCO1	0.927
RCO2	0.952
RCO3	0.964
RCO4	0.899
RCO5	0.911

Notes: Extraction method: principal component analysis; [a] 1 components extracted

Impact

Table AIX. KMO and Bartlett's test

KMO measure of sampling adequacy	0.744
Bartlett's Test of Sphericity	
Approximate chi-square	797.196
df	6
Significance	0.000

Table AX. Component matrix[a]

	Component 1
ICO1	0.796
ICO2	0.751
ICO3	0.891
ICO4	0.787

Notes: Extraction method: principal component analysis; [a] 1 components extracted

Cyberterrorism Knowledge

Table AXI. KMO and Bartlett's test

KMO measure of sampling adequacy	0.853
Bartlett's Test of Sphericity	
Approximate chi-square	2,452.266
df	10
Significance	0.000

Table AXII. Component matrix[a]

	Component 1
KCY1	0.911
KCY2	0.818
KCY3	0.936
KCY4	0.913
KCY5	0.884

Notes: Extraction method: principal component analysis; [a] 1 components extracted

Awareness

Table AXIII. KMO and Bartlett's test

KMO measure of sampling adequacy	0.848
Bartlett's Test of Sphericity	
Approximate chi-square	3,745.137
df	10
Significance	0.000

Table AXIV. Component matrix[a]

	Component 1
ACY1	0.877
ACY2	0.959
ACY3	0.932
ACY4	0.943
ACY5	0.979

Notes: Extraction method: principal component analysis; [a] 1 components extracted

Vulnerabilities

Table AXV. KMO and Bartlett's test

KMO measure of sampling adequacy	0.938
Bartlett's Test of Sphericity	
Approximate chi-square	6,026.609
df	21
Significance	0.000

Table AXVI. Component matrix[a]

	Component 1
VCY1	0.954
VCY2	0.944
VCY3	0.942
VCY4	0.967
VCY5	0.955
VCY6	0.922
VCY7	0.933

Notes: Extraction method: principal component analysis; [a] 1 components extracted

Response

KMO measure of sampling adequacy	0.861
Bartlett's Test of Sphericity	
Approximate chi-square	4,870.149
df	15
Significance	0.000

Table AXVII. KMO and Bartlett's test

	Component 1
RCY1	0.933
RCY2	0.946
RCY3	0.938
RCY4	0.964
RCY5	0.892
RCY6	0.893

Notes: Extraction method: principal component analysis; [a] 1 components extracted

Table AXVIII. Component matrix[a]

Impact

KMO measure of sampling adequacy	0.866
Bartlett's Test of Sphericity	
Approximate chi-square	4,346.413
df	10
Significance	0.000

Table AXIX. KMO and Bartlett's test

	Component 1
ICY1	0.978
ICY2	0.962
ICY3	0.954
ICY4	0.951
ICY5	0.941

Notes: Extraction method: principal component analysis; [a] 1 components extracted

Table AXX. Component matrix[a]

Appendix 2

Table AXXI.
CFA using AMOS.20

Construct	No. of items	CMIN/DF	df	*p*	GFI	CFI	AGFI	SRMR	RMSEA	PCLOSE
Conventional terrorism										
Knowledge	5	3.490	1	0.062	0.997	0.999	0.960	0.003	0.070	0.233
Awareness	5	1.665	1	0.197	0.999	1.000	0.981	0.001	0.036	0.446
Vulnerabilities	3		0		1.000	1.000		0.000	0.763	0.000
Response	5	0.290	4	0.885	0.999	1.000	0.997	0.000	0.000	0.986
Impact	4	0.512	1	0.474	1.000	1.000	0.995	0.001	0.000	0.695
Cyberterrorism										
Knowledge	5	0.846	4	0.496	0.997	1.000	0.990	0.002	0.000	0.884
Awareness	5	3.649	2	0.26	0.994	0.999	0.958	0.002	0.72	0.198
Vulnerabilities	7	1.308	6	0.249	0.999	1.000	0.980	0.001	0.024	0.813
Response	6	0.046	3	0.987	1.000	1.000	0.999	0.000	0.000	0.998
Impact	5	3.256	3	0.21	0.993	0.998	0.964	0.066	0.066	0.227

Appendix 3

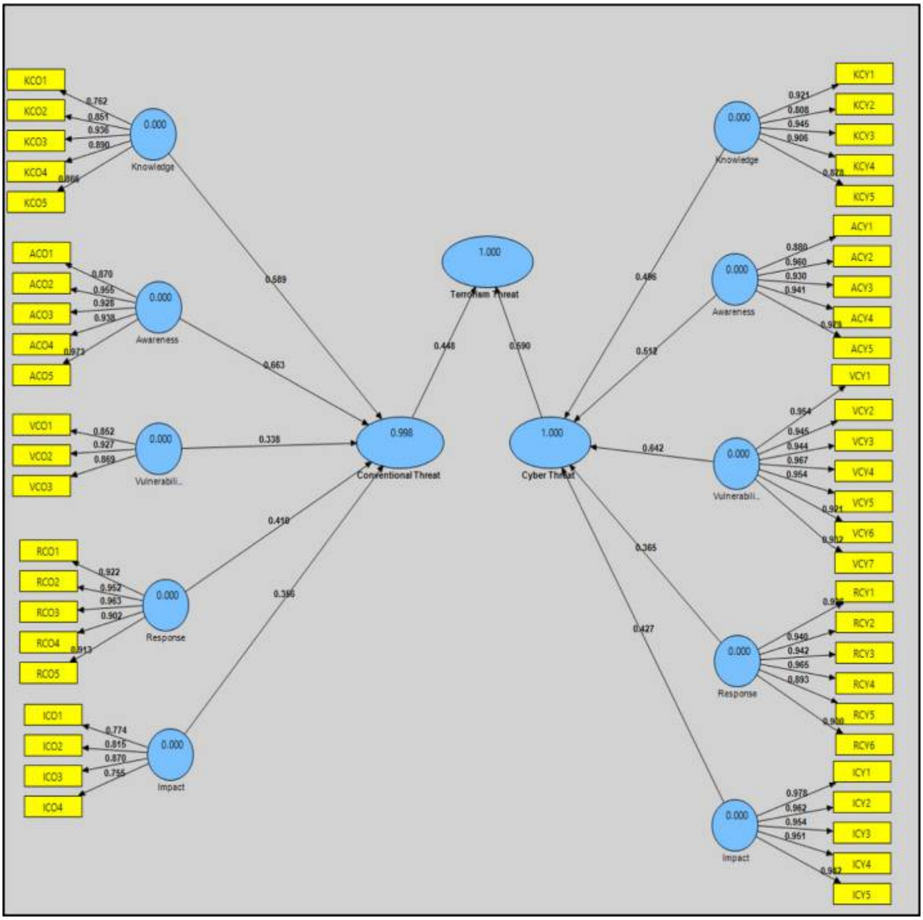

Figure A1.
The full model of the study

Corresponding author
Abdulrahman Alqahtani can be contacted at: qahtaniasa@me.com